ARKIV FÖR MATEMATIK Band 1 nr 38

Communiqué le 6 juin 1951

Sur le plus petit non-reste quadratique impair

Par TRYGVE NAGELL

§ 1.

Soit p un nombre premier >2. Désignons par ψ le plus petit nombre impair positif qui est un non-reste quadratique modulo p. C'est évident que ψ est toujours un nombre premier.

Dans une note [1] publiée en 1923 j'ai proposé le problème de déterminer une borne supérieure de ψ en fonction de p, et par des raisonnements très simples j'y ai démontré que

$$\psi < 2\sqrt{p} + 1 \tag{1}$$

pour tous les nombres premiers $p > 3$.

Ensuite, par des moyens analytiques, J. M. VINOGRADOV a établi le résultat plus précis que voici [2]:

Si p est un nombre premier suffisamment grand tel que $p \equiv \pm 1 \pmod 8$, on a

$$\psi < p^{\nu} (\log p)^2, \tag{2}$$

où $\nu = \dfrac{1}{2\sqrt{e}} = 0.303\ldots$

Enfin, par une méthode élémentaire, A. BRAUER a obtenu le résultat suivant [3]:

Pour tous les nombres premiers $p \equiv \pm 3 \pmod 8$ on a

$$\psi < 2(4p)^{\frac{2}{5}} + 2(4p)^{\frac{1}{5}} + 1. \tag{3}$$

Pour tous les nombres premiers $p \equiv -1 \pmod 8$ on a

$$\psi < (2p)^{\frac{2}{5}} + 3(2p)^{\frac{1}{5}} + 1. \tag{4}$$

J'ai montré récemment comment on peut employer un théorème d'AXEL THUE pour trouver une borne supérieure de ψ. Il s'agit du théorème suivant [4]:

Soit p un nombre premier impair. Si le nombre entier a n'est pas divisible par p, on peut trouver deux nombres entiers positifs x et $y < \sqrt{p}$ et tels qu'on ait

$$ay \equiv \pm x \pmod p$$

pour l'un ou l'autre des deux signes.

Au moyen de ce théorème j'ai établi l'inégalité

$$\psi < \sqrt{p} \tag{5}$$

pour tous les nombres premiers $p \equiv \pm 1 \pmod 8$, sauf pour $p = 7$ et $p = 23$; voir [5] et [6].

Ce résultat n'est pas aussi précis que les inégalités (2) et (4), mais la méthode de démonstration est élémentaire et très simple.

Dans cette Note nous allons développer une nouvelle méthode beaucoup plus simple que toutes les méthodes employées jusqu'ici pour établir le résultat (5) et des résultats analogues.

§ 2.

Supposons d'abord que $p \equiv 1 \pmod 8$. Alors on aura en divisant p par 2ψ

$$p = 2\psi k \pm \varrho,$$

où ϱ est un entier positif $\leqq \psi - 2$. Il en résulte que ϱ est un reste quadratique modulo p. Il faut donc que k soit un non-reste quadratique modulo p. On en conclut que $k \geqq \psi$ et que

$$p \geqq 2\psi^2 - \psi + 2,$$

d'où

$$\psi \leqq \tfrac{1}{4} + \tfrac{1}{4}\sqrt{8p - 15}. \tag{6}$$

Cette inégalité, qui est valable pour tous les nombres premiers $p \equiv 1 \pmod 8$, est plus précise que (5). Nous allons la préciser encore en démontrant que

$$\psi \leqq \sqrt{\tfrac{1}{2}(p + 1)}. \tag{7}$$

Vu que cette inégalité est vraie pour $p = 17$, nous pouvons supposer que $\psi \geqq 5$. En posant

$$p = 2\psi^2 - \psi + 2 + 2a,$$

où a est un entier $\geqq 0$, nous aurons

$$p - (2a + 3)\psi = 2(\psi - 1)(\psi - 1 - a). \tag{8}$$

Supposons maintenant que a soit $\leqq \tfrac{1}{2}(\psi - 5)$. Dans ce cas on aura $2a + 3 \leqq \psi - 2$. Il en résulte que $(2a + 3)\psi$ est un non-reste quadratique modulo p. Or, cela est impossible puisque le second membre de (8) est un reste quadratique modulo p. Il faut donc que $a \geqq \tfrac{1}{2}(\psi - 3)$. Alors on a

$$p \geqq 2\psi^2 - \psi + 2 + \psi - 3 = 2\psi^2 - 1,$$

d'où l'on obtient (7).

§ 3.

La même méthode s'applique dans le cas d'un nombre premier $p \equiv -1 \pmod 8$. En divisant p par ψ nous aurons

$$p = \psi k - r,$$

où r est un entier positif $\leqq \psi - 1$. Il en résulte que r est un reste quadratique modulo p. Donc le nombre k est nécessairement un non-reste quadratique modulo p. Par conséquent on a $k \geqq \psi$ et

$$p \geqq \psi^2 - \psi + 1,$$

d'où

$$\psi \leqq \tfrac{1}{2} + \tfrac{1}{2}\sqrt{4p-3}. \tag{9}$$

Cette inégalité, qui est valable pour tous les nombres premiers $p \equiv -1 \pmod 8$, est moins précise que (5). Si nous supposons que $p > 23$, elle peut être améliorée de la manière suivante. Posons

$$p = \psi^2 - \psi + 1 + a,$$

où $a \geqq 0$. Donc

$$p - a - 3 = (\psi + 1)(\psi - 2).$$

Puisque $\frac{1}{2}(\psi + 1)$ et $\psi - 2$ sont $< \psi$, ces nombres sont des restes quadratiques modulo p; on en conclut que $a + 3$ est un non-reste quadratique modulo p. Donc $a + 3 \geqq \psi$ et

$$p = \psi^2 - \psi + 1 + a \geqq \psi^2 - \psi + 1 + \psi - 3,$$

c'est-à-dire

$$p \geqq \psi^2 - 2.$$

Posons

$$p = \psi^2 - 2 + b.$$

Si $b > 0$, nous aurons

$$p - b + 1 = \psi^2 - 1 = (\psi + 1)(\psi - 1).$$

Vu que $\frac{1}{2}(\psi + 1)$ et $\psi - 1$ sont des restes quadratiques modulo p, il en résulte que $b - 1$ est un non-reste quadratique modulo p. Par conséquent on a $b - 1 \geqq \psi$ et

$$p \geqq \psi^2 - 2 + \psi + 1 = \psi^2 + \psi - 1. \tag{10}$$

Si $b = 0$, nous aurons

$$p - 7 = (\psi + 3)(\psi - 3). \tag{11}$$

Comme $p > 7$, on a $\psi > 3$ et $\frac{1}{2}(\psi + 3) < \psi$. Donc le nombre $\frac{1}{2}(\psi + 3)$ est un reste quadratique modulo p. Alors le second membre de (11) est un reste quadratique modulo p. On en conclut que le nombre 7 est un non-reste quadratique modulo p, c'est-à-dire $\psi \leqq 7$. Donc $p = \psi^2 - 2 \leqq 47$. Or, pour $p = 47$ on a $\psi = 5$; ainsi l'égalité (11) est vrai seulement pour $p = 7$ et $p = 23$.

Donc on conclut de (10): Pour tous les nombres premiers $p \equiv -1 \pmod 8$ on a

$$\psi \leqq -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{4p+5}, \tag{12}$$

sauf pour $p = 7$ et $p = 23$. On voit sans peine que cette inégalité peut être remplacée par la suivante

$$\psi \leqq \sqrt{p-6}. \tag{13}$$

§ 4.

On peut employer une méthode analogue même dans le cas d'un nombre premier $p \equiv 5 \pmod 8$. Mais le raisonnement sera plus compliqué.

En divisant p par ψ nous aurons

$$p = \psi h + r, \tag{14}$$

où h et r sont des entiers positifs, $0 < r < \psi$. Il faut distinguer quatre cas.

1) r est impair, et h est pair. L'un des nombres $-\psi + r$, $-3\psi + r$, $\psi + r$ et $3\psi + r$ est $\equiv 4 \pmod 8$. Si nous désignons ce nombre par r_1, nous avons

$$p = \psi h_1 + r_1, \tag{15}$$

où h_1 est un entier impair, qui a une des valeurs $h + 1$, $h - 1$, $h + 3$, $h - 3$. Les valeurs corréspondantes de r_1 sont $-\psi + r$, $\psi + r$, $-3\psi + r$, $3\psi + r$. Vu que le nombre $\frac{1}{4}|r_1|$ est impair et $< \psi$, r_1 est un reste quadratique modulo p. Il en résulte que h_1 est un non-reste quadratique modulo p. Ainsi h_1 ne peut pas être $= -1$. Donc h_1 est toujours positif et $\geqq \psi$. Par conséquent nous aurons

$$p = \psi h_1 + r_1 \geqq \psi^2 - 3\psi + 1,$$

d'où

$$\psi \leqq \tfrac{3}{2} + \tfrac{1}{2}\sqrt{4p + 5}. \tag{16}$$

2) $r \equiv 4 \pmod 8$; h est impair. Dans ce cas $\frac{r}{4}$ est un reste quadratique impair modulo p; h est un non-reste quadratique impair modulo p. Donc

$$p = \psi h + r \geqq \psi^2 + 4$$

et

$$\psi = \sqrt{p - 4}. \tag{17}$$

3) $r \equiv 0 \pmod 8$; h est impair. Dans ce cas l'équation (14) peut s'écrire

$$p = \psi(h + 4) - (4\psi - r).$$

Le nombre $\psi - \frac{r}{4}$ est un reste quadratique impair modulo p. Donc $h + 4$ est un non-reste quadratique impair modulo p. Par conséquent $h + 4 \geqq \psi$ et

$$p \geqq \psi^2 - 4\psi + 8,$$

d'où

$$\psi \leqq 2 + \sqrt{p - 4}. \tag{18}$$

4) $r \equiv 2 \pmod 4$; h est impair. L'un des nombres $-2\psi + r$ et $2\psi + r$ est $\equiv 4 \pmod 8$. Si nous désignons ce nombre par r_1, nous avons

$$p = \psi h_1 + r_1,$$

où h_1 est ou $= h + 2$ ou $= h - 2$. Les valeurs corréspondantes de r_1 sont $-2\psi + r$ et $2\psi + r$. Vu que le nombre $\frac{1}{4}|r_1|$ est impair et $< \frac{3}{4}\psi$, r_1 est un reste quadratique modulo p. Il en résulte que h_1 est un non-reste quadratique

modulo p. Ainsi h_1 ne peut pas être $= -1$. Donc h_1 est toujours positif et $\geqq \psi$. Par conséquent nous aurons

$$p = \psi h_1 + r_1 \geqq \psi^2 - 2\psi + 2,$$

d'où

$$\psi \leqq 1 + \sqrt{p-1}. \tag{19}$$

Des inégalités (16), (17), (18) et (19) on conclut que

$$\psi \leqq 2 + \sqrt{p-4} \tag{20}$$

pour tous les nombres premiers $p \equiv 5 \pmod 8$.

Remarque. On peut d'ailleurs améliorer le résultat obtenu ci-dessus et démontrer le théorème suivant:

Si p est un nombre premier $\equiv 5 \pmod 8$, on a

$$\psi < \sqrt{p},$$

sauf pour $p = 5$, 13 et 109.

Par une méthode analogue on peut aussi établir le résultat suivant:

Si p est un nombre premier $\equiv 3 \pmod 8$, on a

$$\psi < \sqrt{p} + 4,$$

sauf pour $p = 131$.

*

Dans le tableau suivant p est un nombre premier; ψ désigne le plus petit nombre premier impair tel que $\left(\frac{\psi}{p}\right) = -1$; π désigne le plus petit nombre premier impair tel que $\left(\frac{\pi}{p}\right) = +1$

p	π	ψ	p	π	ψ	p	π	ψ
3	7	5	71	3	7	163	41	3
5	11	3	73	3	5	167	3	5
7	11	3	79	5	3	173	13	3
11	3	7	83	3	5	179	3	7
13	3	5	89	5	3	181	3	7
17	13	3	97	3	5	191	3	7
19	5	3	101	5	3	193	3	5
23	3	5	103	7	3	197	7	3
29	5	3	107	3	5	199	5	3
31	5	3	109	3	11	211	5	3
37	3	5	113	7	3	223	7	3
41	5	3	127	11	3	227	3	5
43	11	3	131	3	17	229	3	7
47	3	5	137	7	3	233	7	3
53	7	3	139	5	3	239	3	7
59	3	11	149	5	3	241	3	7
61	3	7	151	5	3	251	3	11
67	17	3	157	3	5	257	11	3

INDEX BIBLIOGRAPHIQUE. [1] **T. Nagell,** Zahlentheoretische Notizen, Vidensk. selsk. Skrifter, Matem.-naturv. Kl., Oslo 1923. No 13. II. — [2] **J. M. Vinogradov,** On the bound of the least non-residue of *n*th powers, Transactions of the American Mathematical Society 29 (1927), S. 218—226. — [3] **A. Brauer,** Über den kleinsten quadratischen Nichtrest, Mathematische Zeitschrift, 33 (1931), S. 161—176. — [4] **Axel Thue,** Et par antydninger til en talteoretisk methode, Vidensk. selsk. Forhandl., Christiania 1902. No 7. — [5] **T. Nagell,** Sur les restes et les non-restes quadratiques suivant un module premier, Arkiv f. Matematik, Bd 1, Nr 16, Stockholm 1950. — [6] **T. Nagell,** Sur un théorème d'Axel Thue, Arkiv f. Matematik, Bd 1, Nr 36, Stockholm 1951. — [7] **K. Inkeri,** Neue Beweise für einige Sätze zum euklidischen Algorithmus in quadratischen Zahlkörpern, Annales Universitatis Turkuensis, Series A, tom IX, N:o 1, Turku 1948. — [8] **H. J. Kanold,** Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme I, Journal für Mathematik, Bd 187 (1949).

Tryckt den 25 oktober 1951

Uppsala 1951. Almqvist & Wiksells Boktryckeri AB